

Appl. No. 09/822,986
Amdt. Dated 10/13/2005
Reply to Office Action August 23, 2005

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A platform comprising:
a processor; and
a memory coupled to and physically separate from the processor, the memory including an isolated memory area, being a portion of the memory accessible by the processor only when the processor is operating in an isolated execution mode, containing a file checker executable by the processor, the file checker including (i) a file analyzer to perform a scan operation on a file to produce a scanning result and (ii) a signature generator to produce a digital signature chain including a digital signature having the scanning result and a version number of the file analyzer.
2. (Original) The platform of claim 1, wherein the scan operation by the file checker is a virus detection function.
3. (Original) The platform of claim 1 wherein the incoming file is prevented from being executed if the verified digital signature chain indicated an unacceptable file integrity.
4. (Original) The platform of claim 1, wherein the incoming file is accessed if the verified digital signature chain indicates acceptable file integrity.
5. (Currently Amended) The platform of claim 1 further comprising:
a first control unit coupled to both the processor and the memory;
a second control unit coupled to the first control unit; and
a token bus coupled to the second control unit.
6. (Currently Amended) The platform of claim 1, wherein different public and private signatory keys are used for different versions of the file analyzer~~5 further comprising a second control unit coupled to the first control unit and a token bus interface.~~

Appl. No. 09/822,986
Amdt. Dated 10/13/2005
Reply to Office Action August 23, 2005

7. (Currently Amended) The platform of claim 1, wherein the file analyzer to further issue multiple digital certificates with different varying expiration dates ~~6~~ further comprising a non-volatile memory coupled to the second control unit.

8. (Original) The platform of claim 6 further comprising input/output devices coupled to the second control unit.

9. (Original) The platform of claim 2 wherein the file analyzer is one of a virus detector, an intrusion detector, and a file integrity checker.

10. (Original) The platform of claim 1 wherein the signature generator comprises: an encryptor to encrypt the scanning result using a signature key; and a time stamper coupled to the encryptor to time stamp the encrypted result using a time indicator that provides information regarding a recentness of the scan operation, the time stamped encrypted result corresponding to the digital signature.

11. (Previously Presented) The platform of claim 10 wherein the time indicator is one of a calendar time and a version identifier of the scanner.

12. (Previously Presented) The platform of claim 1 wherein the file is code.

13. (Currently Amended) A method comprising:
determining whether a digital signature chain accompanies a file to be accessed;
entering into an isolated execution mode only if the file does not have a corresponding digital signature chain;
analyzing an integrity of the file during the isolated execution mode;
issuing the digital signature chain if the file has an acceptable file integrity during the isolated execution mode; and
verifying the digital signature chain of the file by determining (i) whether the file has an acceptable file integrity, and (ii) whether each signatory providing the digital signature chain is authorized.

Appl. No. 09/822,986
Amdt. Dated 10/13/2005
Reply to Office Action August 23, 2005

14. (Original) The method of claim 13 further comprising:
precluding access to the file if the file has an unacceptable file integrity.

15. (Original) The method of claim 14 further comprising:
precluding access to the file if at least one signatory of the digital signature chain is
unauthorized.

16. (Cancelled).

17. (Previously Presented) The method of claim 13 further comprising:
issuing the digital signature chain with an indication that the file integrity is unacceptable
if the integrity of the file is analyzed and determined to be unacceptable.

18. (Original) The method of claim 13 further comprising:
opening the file if the verified digital signature chain indicates an acceptable file
integrity; and
refusing to open the file if the verified digital signature chain indicates an unacceptable
file integrity.

19. (Currently Amended) A computer program embodied in a processor readable
medium and executable by a processing unit, comprising:
code for determining whether a digital signature chain accompanies a file to be accessed,
and for entering into an isolated execution mode only if the file does not have a corresponding
digital signature chain;
code for issuing the digital signature chain if the file has an acceptable file integrity, the
code for issuing the digital signature chain being stored in protected memory and accessible only
when the processing unit is operating in the isolated execution mode; and
code for verifying the digital signature chain of the file by determining (i) whether the
file has an acceptable file integrity, and (ii) whether each signatory providing the digital
signature chain is authorized.

Appl. No. 09/822,986
Amdt. Dated 10/13/2005
Reply to Office Action August 23, 2005

20. (Original) The method of claim 19 further comprising:
code for precluding access to the file if the file has an unacceptable file integrity.

21. (Original) The method of claim 19 further comprising:
code for precluding access to the file if at least one signatory of the digital signature chain
is unauthorized.

22. (Previously Presented) The method of claim 19, wherein the code for issuing the
digital signature chain further comprising:
code for providing a time stamp to provide timing information related to when a
determination was made whether the digital signature chain accompanies the file to be accessed.

23. (Previously Presented) The method of claim 19, wherein the code for issuing the
digital signature chain further comprising:
code for providing a version number of the code for determining whether the digital
signature chain accompanies the file to be accessed.